I. THE PATENT CLAIMS

1. (Currently amended) A method for auditing the security of a first enterprise including plural computers, where the term enterprise is defined to be a collection of computers, software, and networking that interconnects the computing environment of an organization of people ~~who may be widely distributed geographically~~, comprising:

collecting security information from the computers of the first enterprise under audit;

analyzing the security information and providing a first result of this analysis; and

comparing this first result with a second result comprising information derived from information previously obtained through application of the collecting and analyzing steps to one or more other enterprises that interconnect the computing environments of other different organizations of people ~~who may also be widely distributed~~, these one or more other enterprises together forming a relevant peer group of other different organizations of people, the result of this comparing step indicating the relative security of the first enterprise under audit relative to that of the peer group of one or more other enterprises;

where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these.

2-3. (Cancelled)

4. (Original) The method of claim 1, further comprising the step of generating at least one report that presents the first and second results arranged in a way that facilitates their comparison.

5. (Original) The method of claim 4 wherein the generating step includes presenting the first and second results each broken down into several results relating to several different areas of security, with a first and a second result presented for each different area of security and arranged in a way that facilitates their comparison.

6. (Original) The method of claim 5 wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step.

7. (Original) The method of claim 5 wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of password security information and file access permission security information.

8. (Original) The method of claim 7 wherein, in the generating step, the results relating to several different areas of security further comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step.

9. (Previously presented) The method of claim 5 wherein, in the generating step, the several different areas of security comprise one or more results of analysis of computer configuration security information and one or more results of analysis of security information gathered using interviews.

10. (Previously presented) The method of claim 9 wherein, in the generating step, the one or more results of analysis of computer configuration security information comprise results arising from analysis of password security information.

11. (Previously presented) The method of claim 9 wherein, in the generating step, the one or more results of analysis of computer configuration security information comprises results arising from analysis of file access permission security information.

12. (Original) The method of claim 4, wherein the generating step generates at least two comparative reports in different formats for different requesting parties or uses, and in particular one for technical experts that includes technical language and details and another for non-technical-experts that substantially excludes technical language and details.

13. (Previously presented) The method of claim 1, to which is added:

generating and executing commands to alter the security information of one or more computers to improve system security in at least some cases when the analysis or comparison or both indicate security is in need of improvement.

14. (Original) The method of claim 13, further comprising;

generating at least one report that presents the first and second results arranged in a way that facilitates their comparison.

15. (Original) The method of claim 13 wherein the generating commands step generates commands which force the deactivation or correction of one or more passwords when the analysis or comparison or both indicate that these one or more passwords are not sufficiently secure.

16. (Original) The method of claim 13 wherein the generating commands step generates commands which force alteration of one or more configuration file or control file access permissions if the analysis or comparison or both indicate that the access permissions assigned to these one or more files do not provide adequate system security.

17. (Currently amended) A system for auditing the security of a first enterprise, where the term enterprise is defined to be a collection of computers, software, and networking that interconnects the computing environment of an organization of people ~~who may be widely distributed geographically~~, comprising:

a plurality of computers within the first enterprise under audit;

collectors associated with the computers and arranged to collect from the computers information concerning the security of the first enterprise under audit;

a security analyzer arranged to analyze the information concerning the security of the first enterprise under audit and to provide a first result of this analysis;

a data base containing a second result comprising information derived from information previously obtained through application of the collectors and security analyzer to one or more other enterprises that interconnect the computing environments of other different organizations of people ~~who may also be widely distributed~~, these one or more other enterprises together forming a relevant peer group of other different organizations of people; and

a comparison mechanism arranged to compare the first and second results to determine the relative security of the first enterprise under audit in comparison to that of the one or more enterprises of other different organizations of people in the relevant peer group;

where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these.

18. (Original) A system in accordance with claim 17 to which is added:

a report generator that generates at least one report which presents the first and second results arranged each broken down into several results relating to several different areas of security, with a first and second result presented for each different area of security and arranged in a way that facilitates their comparison.

19. (Previously presented) A system in accordance with claim 17 to which is added:

change agents associated with the computers and able to execute commands that alter computer configuration information; and

a command generator that provides commands to the change agents on selected computers to alter computer configuration information to improve system security in response to the analyzer or comparison mechanism or both determining security improvements are needed.

20. (Original) A system in accordance with claim 19 wherein the command generator includes a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the deactivation or correction of one or more secure passwords if the security analyzer or comparison mechanism or both determine that one or more passwords are not sufficiently secure.

21. (Previously presented) A system in accordance with claim 19 wherein the command generator includes a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the alteration of the access permissions of one or more configuration files or control files if the security analyzer or comparison mechanism or both

determine that the access permissions assigned to one or more such files do not provide sufficient security.

22. (Currently amended) A system for auditing the security of a first enterprise, where the term enterprise is defined to be a collection of computers, software, and networking that interconnects the computing environment of an organization of people ~~who may be widely distributed geographically~~, comprising:

a plurality of computers within the first enterprise under audit;

collector means associated with the computers for collecting information from the computers concerning the security of the first enterprise under audit;

security analyzer means for analyzing the information concerning the security of the first enterprise under audit and for providing a first result of this analysis;

data base means for storing and for presenting a second result comprising information derived from information previously obtained through application of the collector means and security analyzer means to one or more other enterprises that interconnect the computing environments of other different organizations of people ~~who may also be widely distributed~~, these one or more other enterprises together forming relevant peer group of other different organizations of people; and

comparison means for comparing the first and second results to determine the relative security of the first enterprise under audit in comparison to that of the one or more enterprises of other different organizations of people in the relevant peer group;

where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these.

23. (Previously presented) A system in accordance with claim 22 to which is added

report generation means for generating at least one report which presents the first and second results each broken down into several results relating to several different areas of

security, with a first and second result presented for each different area of security and arranged in a way that facilitates their comparison.

24. (Previously presented) A system in accordance with claim 22 to which is added

change agent means associated with the computers for executing commands that alter computer configuration information; and

command generator means for providing commands to the change agent means on selected computers as needed to alter system configuration information to improve system security in response to the security analyzer means or the comparison means or both determining that security improvements are needed.